(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－111649
（P2002－111649A）
(43)公開日　平成14年４月12日(2002.4.12)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｊ１０４
12/56			６０１Ｅ	５Ｋ０３０
		11/20	１０２Ａ	

審査請求　有　　請求項の数９　ＯＬ　（全７頁）

(21)出願番号　特願2000－297847(P2000－297847)

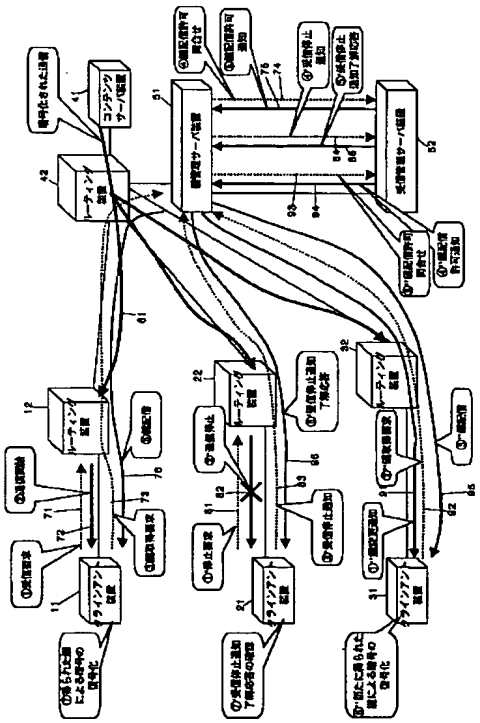
(22)出願日　平成12年９月29日(2000.9.29)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　安藤　大介
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　青柳　慎一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100059258
弁理士　杉村　暁秀　（外１名）

最終頁に続く

(54)【発明の名称】　マルチキャスト通信方法、サーバ装置及びクライアント装置

(57)【要約】
【課題】　ＩＧＭＰを使用するマルチキャスト通信において、マルチキャスト通信データの受信者の管理及び制御を容易に行うことができる方法及び装置を提供する。
【解決手段】　マルチキャストデータを配信するコンテンツサーバ装置、ＩＰレイヤのルーティング装置、暗号化及び復号化鍵を管理する鍵管理サーバ装置、クライアント装置を管理する受信管理サーバ装置、及び、マルチキャストデータを受信するクライアント装置を含み、コンテンツサーバ装置がマルチキャストデータを暗号化してＩＰネットワーク上に配信し、クライアント装置が鍵管理サーバ装置に対して復号化鍵の取得を要求し、鍵管理サーバ装置が受信管理サーバ装置に対して復号化鍵の配信可否を問合わせ、受信管理サーバ装置が復号化鍵の配信を許可し、鍵管理サーバ装置がクライアント装置に対して復号化鍵を配信し、クライアント装置がマルチキャストデータの暗号を復号化する。



1

【特許請求の範囲】

【請求項１】　マルチキャストデータを配信するコンテンツサーバ装置、ＩＰレイヤのルーティング装置、暗号化及び復号化鍵を管理する鍵管理サーバ装置、クライアント装置を管理する受信管理サーバ装置、及び、マルチキャストデータを受信するクライアント装置を含むマルチキャスト通信システムにおけるマルチキャスト通信方法であって、

コンテンツサーバ装置がマルチキャストデータを暗号化してＩＰネットワーク上に配信し、

クライアント装置が、マルチキャストプロトコルの終端点になっているルーティング装置に対して受信要求を行い、

ルーティング装置は、受信要求を受けると、クライアント装置に対してマルチキャストデータを配信し、

クライアント装置は、鍵管理サーバ装置に対して復号化鍵の取得要求を行い、鍵管理サーバ装置は、復号化鍵の取得要求を受けると、受信管理サーバ装置に対して復号化鍵の配信可否の問合わせを行い、

受信管理サーバ装置は、復号化鍵の配信可否の問合わせを受けると、記録されているクライアント装置の受信状況に応じて復号化鍵の配信許可通知を行うと共に受信情報を保持し、

鍵管理サーバ装置は、復号化鍵の配信許可通知を受けると、クライアント装置に対して復号化鍵の配信を行い、

クライアント装置は、復号化鍵の配信を受けると、この復号化鍵を利用して、配信されているマルチキャストデータの暗号の復号化を行うことを特徴とするマルチキャスト通信方法。

【請求項２】　マルチキャストデータを配信するコンテンツサーバ装置、ＩＰレイヤのルーティング装置、暗号化及び復号化鍵を管理する鍵管理サーバ装置、クライアント装置を管理する受信管理サーバ装置、及び、マルチキャストデータを受信するクライアント装置を含むマルチキャスト通信システムにおけるマルチキャスト通信方法であって、

マルチキャスト通信を停止する場合、

クライアント装置が、マルチキャストプロトコルの終端点になっているルーティング装置に対して受信停止要求を行い、

ルーティング装置は、受信停止要求を受けると、クライアント装置に対してマルチキャストデータの配信の停止を行い、

クライアント装置は、鍵管理サーバ装置に対して受信停止通知を行い、

鍵管理サーバ装置は、クライアント装置から受信停止通知を受けると、受信管理サーバ装置に対して受信停止通知を行い、

受信管理サーバ装置は、受信停止通知を受けると、保持されているクライアント装置の受信情報を削除し、受信状態の記録を行い、鍵管理サーバ装置に対して受信停止通知了解応答を行い、

鍵管理サーバ装置は、受信停止通知了解応答を受けると、クライアント装置に対して受信停止通知了解応答を行い、

クライアント装置は、受信停止通知了解応答を受けて受信停止の確認を行うことを特徴とするマルチキャスト通信方法。

2

【請求項３】　マルチキャストデータを配信するコンテンツサーバ装置、ＩＰレイヤのルーティング装置、暗号化及び復号化鍵を管理する鍵管理サーバ装置、クライアント装置を管理する受信管理サーバ装置、及び、マルチキャストデータを受信するクライアント装置を含むマルチキャスト通信システムにおけるマルチキャスト通信方法であって、

復号化鍵を変更する場合、

コンテンツサーバ装置が暗号化鍵の変更を行い、その変更内容を鍵管理サーバ装置に通知し、

鍵管理サーバ装置がその内容を保持し、クライアント装置に対して復号化鍵の変更通知を行い、

クライアント装置は、復号化鍵の変更通知を受けると、鍵管理サーバ装置に対して復号化鍵の取得要求を行い、変更後の復号化鍵を取得することを特徴とするマルチキャスト通信方法。

【請求項４】　ＩＰを利用するマルチキャスト通信システムにおける暗号化及び復号化鍵を管理するための鍵管理サーバ装置であって、

クライアント装置の復号化鍵の取得要求に応じるための手段、

受信管理サーバ装置に対してクライアント装置への復号化鍵の配信の可否を問合わせるための手段、

受信管理サーバ装置の応答に応じて復号化鍵を配信するための手段、

クライアント装置からマルチキャストデータの受信停止通知を受信するための手段、

受信管理サーバ装置に対してクライアント装置の受信停止通知を行うための手段、

受信管理サーバ装置から受信停止通知了解応答を受信するための手段、及び、クライアント装置に対して受信停止通知了解応答を行うための手段を具えることを特徴とするサーバ装置。

【請求項５】　ＩＰを利用するマルチキャスト通信システムにおけるクライアント装置の受信を管理するための受信管理サーバ装置であって、

鍵管理サーバ装置のクライアント装置への鍵の配信可否の問合わせに応じるための手段、

問合わせ内容に応じてクライアント装置の情報を保持するための手段、

鍵管理サーバ装置からクライアント装置の受信停止通知を受信するための手段、

鍵管理サーバ装置へ受信停止通知了解応答を行うための手段、
受信停止通知に応じてクライアント装置の保持情報を削除するための手段、及び、
受信停止通知に応じて受信状況を記録するための手段を具えることを特徴とするサーバ装置。

【請求項６】　ＩＰを利用するマルチキャスト通信システムにおける暗号化及び復号化鍵を管理し、且つ、ＩＰを利用するマルチキャスト通信システムにおけるクライアント装置の受信を管理するためのサーバ装置であって、請求項４及び５に記載の各手段を具えることを特徴とするサーバ装置。

【請求項７】　請求項４又は６に記載のサーバ装置において、更に、
暗号化鍵を一定時間毎に更新するための手段、
更新された暗号化鍵を保持するための手段、及び、
更新内容に応じてマルチキャストデータを受信しているクライアント装置に復号化鍵の変更の通知を行うための手段を具えることを特徴とするサーバ装置。

【請求項８】　ＩＰを利用するマルチキャスト通信システムにおけるクライアント装置であって、
受信要求を送出するための手段、
鍵管理サーバ装置に対して復号化鍵の取得要求を行うための手段、
得られた復号化鍵を利用してマルチキャストデータの復号化を行うための手段、
受信停止要求を送出するための手段、
鍵管理サーバ装置に対して受信停止通知を行うための手段、及び、
鍵管理サーバ装置から受信停止通知了解応答を受信するための手段を具えることを特徴とするクライアント装置。

【請求項９】　請求項８に記載のクライアント装置において、更に、
鍵管理サーバ装置から復号化鍵の変更通知を受信するための手段、及び、該変更通知に応じて、鍵管理サーバ装置に対して復号化鍵の取得要求を行うための手段を具えることを特徴とするクライアント装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ルーティング装置、スイッチ等を利用するＩＰネットワークにおけるデータ通信に関するものであり、特に、ポイント対マルチポイント通信であるマルチキャスト通信の通信方法及び装置に関するものである。

【０００２】

【従来の技術】ＩＰネットワークにおいてポイント対マルチポイント通信を行う場合、ブロードキャスト、マルチキャスト等の技術を使用することができる。特にマルチキャストを使用する場合、受信希望者のみにデータを送信することができ、帯域の有効利用を図ることができる。このマルチキャストを実現するプロトコルとしては、送信側ベースのプロトコル及び受信側ベースのプロトコルがある。しかしながら、送信側ベースのプロトコルは殆どのルーティング装置及びレイヤ３のスイッチに実装されていないため、マルチキャスト通信を行う場合、受信側ベースマルチキャストプロトコルＩＧＭＰを使用する場合が多い。

【０００３】図１はＩＧＭＰを使用するマルチキャスト通信方法を説明するための図である。データを受信する場合は、例えば受信を希望するクライアント装置111がＩＧＭＰの終端点となっているルーティング装置112に対して受信要求142を行い、ルーティング装置112がデータの送信143を開始する。また、データの受信を停止する場合は、例えば受信の停止を希望するクライアント装置121がＩＧＭＰの終端点となっているルーティング装置122に対して停止要求144を行い、ルーティング装置122がデータの送信を停止145する。

【０００４】このように、ＩＧＭＰを使用する方法においては、クライアントの受信要求及び停止要求は共にＩＧＭＰの終端ルーティング装置に対して行うため、送信側のサーバでは通信の管理を行う必要がない。このような方法は、スケーラビリティを考慮する上では有効な方法といえる。

【０００５】しかしながら、サーバ側では管理を行わないのでデータ受信を行っているクライアントを把握できない。また、ＩＧＭＰ自体が受信管理を行う機能を持っておらず、一方、ＩＧＭＰルーティング装置は受信クライアントを管理しているが、実際にはクライアントを特定して管理するのではなく、クライアントが所属するサブネットを管理しているため、クライアントの特定は不可能である。このように、ＩＧＭＰを使用するマルチキャスト通信では、データ受信者の管理及び制御が難しいため、例えば、課金処理を行うことが困難であるという問題があった。

【０００６】

【発明が解決しようとする課題】本発明の目的は、上述の問題点に鑑み、ＩＧＭＰを使用するマルチキャスト通信において、マルチキャスト通信データの受信者の管理及び制御を容易に行うことができる方法及び装置を提供することにある。

【０００７】

【課題を解決するための手段】本発明のマルチキャスト通信方法は、マルチキャストデータを配信するコンテンツサーバ装置、ＩＰレイヤのルーティング装置、暗号化及び復号化鍵を管理する鍵管理サーバ装置、クライアント装置を管理する受信管理サーバ装置、及び、マルチキャストデータを受信するクライアント装置を含むマルチキャスト通信システムにおけるマルチキャスト通信方法であって、コンテンツサーバ装置がマルチキャストデー

タを暗号化してＩＰネットワーク上に配信し、クライアント装置が、マルチキャストプロトコルの終端点になっているルーティング装置に対して受信要求を行い、ルーティング装置は、受信要求を受けると、クライアント装置に対してマルチキャストデータを配信し、クライアント装置は、鍵管理サーバ装置に対して復号化鍵の取得要求を行い、鍵管理サーバ装置は、復号化鍵の取得要求を受けると、受信管理サーバ装置に対して復号化鍵の配信可否の問合わせを行い、受信管理サーバ装置は、復号化鍵の配信可否の問合わせを受けると、記録されているクライアント装置の受信状況に応じて復号化鍵の配信許可通知を行うと共に受信情報を保持し、鍵管理サーバ装置は、復号化鍵の配信許可通知を受けると、クライアント装置に対して復号化鍵の配信を行い、クライアント装置は、復号化鍵の配信を受けると、この復号化鍵を利用して、配信されているマルチキャストデータの暗号の復号化を行うことを特徴とする。

【０００８】また、本発明のマルチキャスト通信方法は、マルチキャスト通信を停止する場合、クライアント装置が、マルチキャストプロトコルの終端点になっているルーティング装置に対して受信停止要求を行い、ルーティング装置は、受信停止要求を受けると、クライアント装置に対してマルチキャストデータの配信の停止を行い、クライアント装置は、鍵管理サーバ装置に対して受信停止通知を行い、鍵管理サーバ装置は、クライアント装置から受信停止通知を受けると、受信管理サーバ装置に対して受信停止通知を行い、受信管理サーバ装置は、受信停止通知を受けると、保持されているクライアント装置の受信情報を削除し、受信状態の記録を行い、鍵管理サーバ装置に対して受信停止通知了解応答を行い、鍵管理サーバ装置は、受信停止通知了解応答を受けると、クライアント装置に対して受信停止通知了解応答を行い、クライアント装置は、受信停止通知了解応答を受けて受信停止の確認を行うことを特徴とする。

【０００９】また、本発明のマルチキャスト通信方法は、復号化鍵を変更する場合、コンテンツサーバ装置が暗号化鍵の変更を行い、その変更内容を鍵管理サーバ装置に通知し、鍵管理サーバ装置がその内容を保持し、クライアント装置に対して復号化鍵の変更通知を行い、クライアント装置は、復号化鍵の変更通知を受けると、鍵管理サーバ装置に対して復号化鍵の取得要求を行い、変更後の復号化鍵を取得することを特徴とする。

【００１０】更に、本発明のＩＰを利用するマルチキャスト通信システムにおける暗号化及び復号化鍵を管理するための鍵管理サーバ装置は、クライアント装置の復号化鍵の取得要求に応じるための手段、受信管理サーバ装置に対してクライアント装置への復号化鍵の配信の可否を問合わせるための手段、受信管理サーバ装置の応答に応じて復号化鍵を配信するための手段、クライアント装置からマルチキャストデータの受信停止通知を受信するための手段、受信管理サーバ装置に対してクライアント装置の受信停止通知を行うための手段、受信管理サーバ装置から受信停止通知了解応答を受信するための手段、及び、クライアント装置に対して受信停止通知了解応答を行うための手段を具えることを特徴とする。

【００１１】また、本発明の鍵管理サーバ装置は、更に、暗号化鍵を一定時間毎に更新するための手段、更新された暗号化鍵を保持するための手段、及び、更新内容に応じてマルチキャストデータを受信しているクライアント装置に復号化鍵の変更の通知を行うための手段を具えることができる。

【００１２】更に、本発明のＩＰを利用するマルチキャスト通信システムにおけるクライアント装置の受信を管理するための受信管理サーバ装置は、鍵管理サーバ装置のクライアント装置への鍵の配信可否の問合わせに応じるための手段、問合わせ内容に応じてクライアント装置の情報を保持するための手段、鍵管理サーバ装置からクライアント装置の受信停止通知を受信するための手段、鍵管理サーバ装置へ受信停止通知了解応答を行うための手段、受信停止通知に応じてクライアント装置の保持情報を削除するための手段、及び、受信停止通知に応じて受信状況を記録するための手段を具えることを特徴とする。

【００１３】更に、本発明のＩＰを利用するマルチキャスト通信システムにおけるクライアント装置は、受信要求を送出するための手段、鍵管理サーバ装置に対して復号化鍵の取得要求を行うための手段、得られた復号化鍵を利用してマルチキャストデータの復号化を行うための手段、受信停止要求を送出するための手段、鍵管理サーバ装置に対して受信停止通知を行うための手段、及び、鍵管理サーバ装置から受信停止通知了解応答を受信するための手段を具えることを特徴とする。

【００１４】また、本発明のクライアント装置は、更に、鍵管理サーバ装置から復号化鍵の変更通知を受信するための手段、及び、変更通知に応じて、鍵管理サーバ装置に対して復号化鍵の取得要求を行うための手段を具えることができる。

【００１５】

【発明の実施の形態】次に、本発明の実施例を説明する。図２は本発明の実施例を説明するための図であり、受信側ベースマルチキャストプロトコルＩＧＭＰを使用するコンテンツ配信ＩＰネットワークの構成を示す図である。図に示されたＩＰネットワークには、マルチキャストデータを配信するコンテンツサーバ装置41、ＩＰレイヤのルーティング装置12、22、32、42、暗号化及び復号化鍵を管理する鍵管理サーバ装置51、クライアント装置を管理する受信管理サーバ装置52、マルチキャストデータを受信するクライアント装置11、21、31が含まれている。マルチキャストデータは、暗号化されて、コンテンツサーバ装置41からＩＰネットワーク内に配信61され

る。

【００１６】次に、例えばクライアント装置11が、マルチキャストデータを受信する場合の動作を説明する。クライアント装置11が、マルチキャストプロトコルの終端点になっているルーティング装置12に対して受信要求71を行う。ルーティング装置12は、受信要求を受けると、クライアント装置11に対してマルチキャストデータの配信72を開始する。その後、クライアント装置11は、鍵管理サーバ装置51に対して復号化鍵の取得要求73を行う。鍵管理サーバ装置51は、復号化鍵の取得要求を受けると、受信管理サーバ装置52に対して復号化鍵の配信可否の問い合わせ74を行う。受信管理サーバ装置52は、復号化鍵の配信可否の問い合わせを受けると、記録されているクライアント装置11の受信状況に応じて復号化鍵の配信許可通知75を行うと共に受信情報を保持する。受信管理サーバ装置52は、復号化鍵の配信許可通知を受けると、クライアント装置11に対して復号化鍵の配信76を行う。クライアント装置11は、復号化鍵の配信を受けると、この復号化鍵を利用して、配信されているマルチキャストデータの暗号の復号化を行う。

【００１７】次に、例えばクライアント装置21が、受信しているマルチキャストデータの受信停止を行う場合の動作を説明する。クライアント装置21が、マルチキャストプロトコルの終端点になっているルーティング装置22に対して受信停止要求81を行う。ルーティング装置22は、受信停止要求を受けると、クライアント装置21に対してマルチキャストデータの配信の停止82を行う。その後、クライアント装置21は、鍵管理サーバ装置51に対して受信停止通知83を行う。鍵管理サーバ装置51は、クライアント装置21から受信停止通知を受けると、受信管理サーバ装置52に対して受信停止通知84を行う。受信管理サーバ装置52は、受信停止通知を受けると、保持されているクライアント装置21の受信情報を削除し、受信状態の記録を行い、鍵管理サーバ装置51に対して受信停止通知了解応答85を行う。鍵管理サーバ装置51は、受信停止通知了解応答を受けると、クライアント装置21に対して受信停止通知了解応答86を行う。クライアント装置21は、受信停止通知了解応答を受けて受信停止の確認を行う。

【００１８】次に、マルチキャストデータを暗号化及び復号化鍵を変更する場合の動作を説明する。暗号化及び復号化鍵の変更は、例えば一定時間毎に、コンテンツサーバ装置が行い、その変更内容を鍵管理サーバ装置に通知し、鍵管理サーバ装置がその内容を保持する。例えばクライアント装置31が、復号化鍵の変更が行われるマルチキャストデータを受信しているとする。鍵管理サーバ装置51が、クライアント装置31に対して復号化鍵の変更通知91を行う。クライアント装置31は、復号化鍵の変更通知を受けると、鍵管理サーバ装置51に対して復号化鍵の取得要求92を行う。鍵管理サーバ装置51は、復号化鍵の取得要求を受けると、受信管理サーバ装置52に対して復号化鍵の配信可否の問い合わせ93を行う。受信管理サーバ装置52は、復号化鍵の配信可否の問い合わせを受けると、記録されているクライアント装置31の受信状況に応じて復号化鍵の配信許可通知94を行うと共に受信情報を保持する。受信管理サーバ装置52は、復号化鍵の配信許可通知を受けると、クライアント装置31に対して復号化鍵の配信95を行う。クライアント装置31は、復号化鍵の配信を受けると、新たに得られたこの復号化鍵を利用して、配信されているマルチキャストデータの暗号の復号化を行う。

【００１９】以上の例によれば、鍵管理サーバ装置及び受信管理サーバ装置が、マルチキャストデータのマルチキャストプロトコルの受信要求、受信停止要求及び復号化鍵の取得要求を受付けて処理することにより、これらの装置によりクライアント装置の受信状況の管理及び制御を行うことが可能になる。

【００２０】上述の例では、ＩＰネットワークが各１台のコンテンツサーバ装置、鍵管理サーバ装置及び受信管理サーバ装置を含む場合を示したが、ＩＰネットワークがこれらの装置を複数含んでいてもよいことは勿論である。また、３台のクライアント装置及び４台のルーティング装置を示したが、この数は限定されないことも勿論である。また、マルチキャストプロトコルの終端点にあるルーティング装置配下には各１台のクライアント装置が接続されている例を示したが、この数は限定されないことも勿論である。また、上述では鍵管理サーバ装置と受信管理サーバ装置とが別装置である例を説明したが、両者の機能を含むサーバ装置としてもよいことは勿論である。

【００２１】更に、本発明は、ルーティング装置相互間、ルーティング装置とクライアント装置との間、ルーティング装置とコンテンツサーバ装置との間、ルーティング装置と鍵管理サーバ装置との間、及び、鍵管理サーバ装置と受信管理サーバ装置との間の通信線、通信方法及び通信装置には依存しない。また、コンテンツサーバ装置から配信されるコンテンツは、ブロックデータ、ストリーム等、どのような種類のデータであってもよい。また、クライアント装置における、マルチキャストプロトコルによる受信要求と復号化鍵の取得要求との順序は、上述の例に限定されるものではなく任意に定めることができる。同様に、クライアント装置における、マルチキャストプロトコルによる受信停止要求と鍵管理サーバ装置への受信停止通知との順序は、上述の例に限定されるものではなく任意に定めることができる。

【００２２】

【発明の効果】以上説明したように、本発明によれば、マルチキャスト通信において、受信側ベースのマルチキャストプロトコルを使用し、暗号化及び復号化を管理する鍵管理サーバを組合せることにより、従来不可能であ

ったマルチキャスト通信データの受信者に関する管理及び制御が可能になる。

【図面の簡単な説明】

【図１】　ＩＧＭＰを使用するマルチキャスト通信方法を説明するための図である。

【図２】　本発明の実施例を説明するための図である。

【符号の説明】

１１、２１、３１　クライアント装置

１２、２２、３２、４２　ルーティング装置

４１　コンテンツサーバ装置

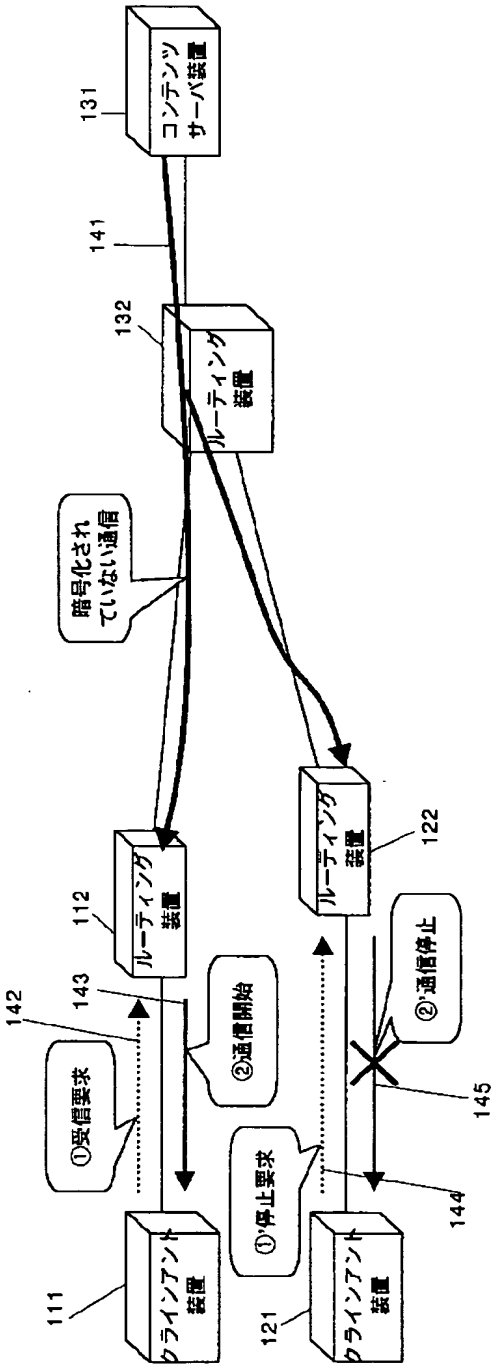
５１　鍵管理サーバ装置

５２　受信管理サーバ装置

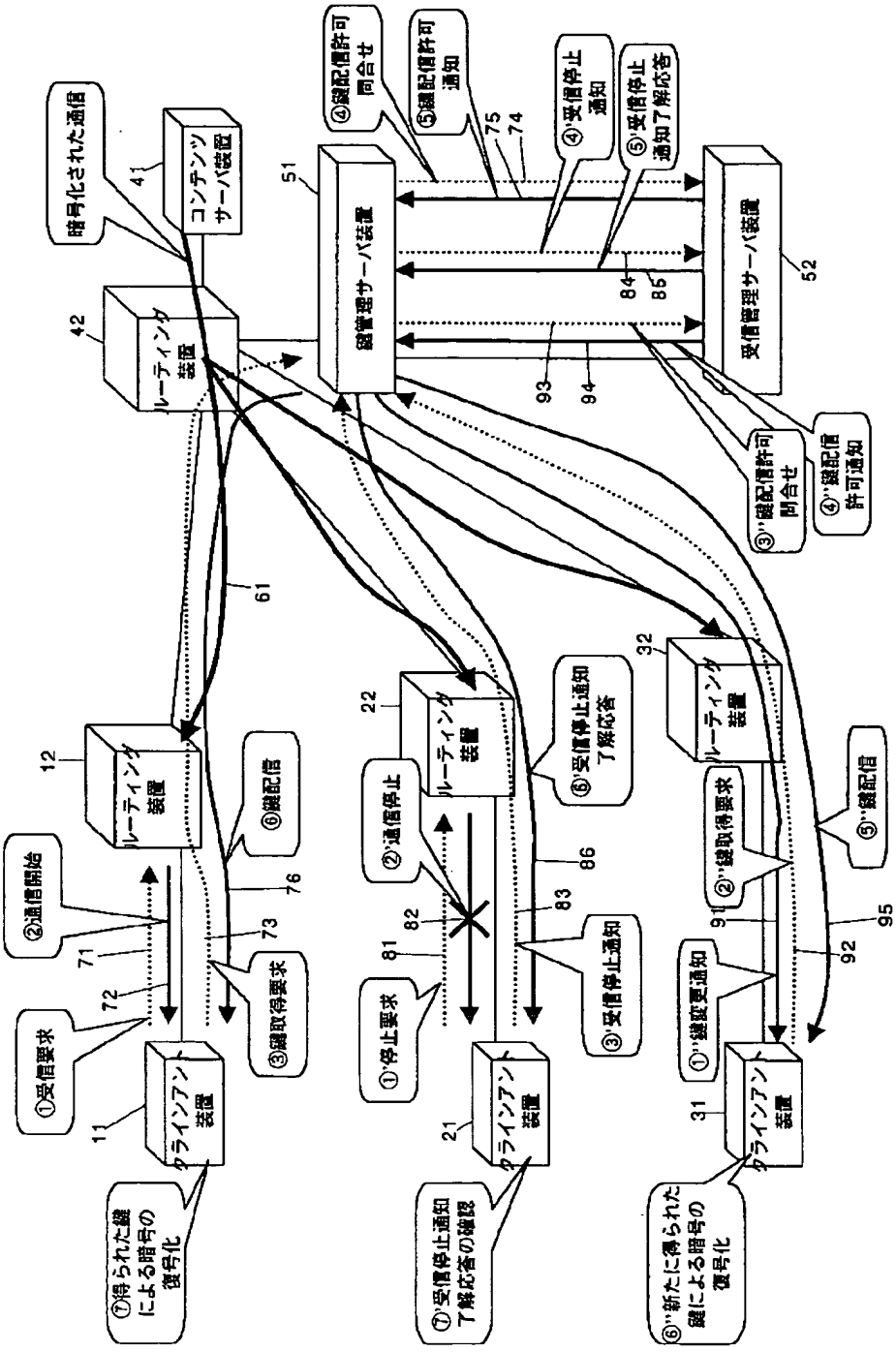
１１１、１２１、１３１　クライアント装置

１１２、１２２、１３２　ルーティング装置

【図１】



【図２】



フロントページの続き

(72)発明者　家永　憲人
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5J104 AA01 AA16 EA01 EA04 EA16 MA08 NA02 PA11
5K030 GA15 HA08 HD03 KA06 KX28 LB02 LB03 LD05